

SECURE EQUIPMENT ACQUISITION POLICY TASK FORCE
THREAT ANALYSIS/ASSESSMENT SUBCOMMITTEE

ASSUMPTIONS:

o By their nature, computer systems bring together a series of security vulnerabilities.

✓(a) There is extensive human intervention throughout the entire life cycle of modern data processing and communications systems. Since the security safeguards protecting these systems are susceptible to accidental or deliberate human intervention, the trust and confidence we place in the people who build, operate, access, maintain and service the equipment and operating systems is an indispensable element of any security program.

(b) Significant hardware and firmware vulnerabilities are shared among the computer, the communications mediums and the remote devices. Likewise, there are potential security vulnerabilities at all levels of the machine operating system and supporting software.

✓(c) There are vulnerabilities in the organization of the physical, technical and procedural security mechanisms protecting the equipment and its environment throughout its life cycle.

o Each of these vulnerabilities cited above can be broadly defined as the dangers of accidental disclosures, physical attacks and deliberate penetrations. Of these three major categories, the threat posed by a sophisticated technical penetration is the most difficult to predict and to detect, and therefore the most difficult to defend against.

o Deliberate penetration is defined as a conscious attempt to obtain information contained in the system; to cause the system to operate to the advantage of the threatening party; or to manipulate the system so as to render it unreliable or unuseable to the legitimate operators.

o Deliberate efforts to penetrate secure systems can include both active infiltration - such as attempts to defeat hardware or software controls - or passive methods - such as bugging or monitoring electromagnetic emanations.

o The principal threat [for the purposes of this working group] will be assumed to be intentional acts perpetrated by an enemy who is rational, highly motivated, has unlimited resources and who has a level of technical knowledge and capability equal to that of his potential victim.

Page Denied

Next 3 Page(s) In Document Denied